UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/644,297	08/20/2003	Naveen Aerrabotu	CS23215RL	6653

20280 7590 05/04/2007

MOTOROLA INC
600 NORTH US HIGHWAY 45
ROOM AS437
LIBERTYVILLE, IL 60048-5343

EXAMINER	
MOUTAOUAKIL, MOUNIR	

ART UNIT	PAPER NUMBER
2616	

MAIL DATE	DELIVERY MODE
05/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/644,297	**Applicant(s)** AERRABOTU ET AL.	
	Examiner Mounir Moutaouakil	**Art Unit** 2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 August 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 August 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Specification

1. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 8 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 8, line 1, "the network gateway" lacks antecedent basis.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) The invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-6, 9-18, 20-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Donahue (US 2003/0123465).

Regarding claim 1, Donahue discloses a method of controlling packet data traffic between a wireless network and a wireless device on a primary link (see figure 2, see page 3, paragraph [0045]. The system is configured to control data traffic between a wireless network and a wireless device like a PDA or cellphone), the method comprises setting primary link traffic flow template filter parameters at a packet control module (see figure 3 and page 4, paragraphs 51-53. the packet control module discloses a filtering data base which functions as a traffic flow template); comparing incoming packet data against the primary link traffic flow template filter parameters; and controlling how the incoming packet data is sent to the wireless device over the primary link based on comparing incoming packet data against the primary link traffic flow template filter parameters (see page 5, paragraphs 61-64. the IP device determines the filtering level that need to be applied based on the client device, by comparing IP addresses 328(1)-(N), see figure 3. The IP device adds source routing details so that incoming data will get filtered depending on the filtering level required by the client).

Regarding claim 2. Donahue discloses a method of controlling packet data traffic, which further comprises receiving a primary packet data protocol link request message including a traffic flow template information element (see figure 3 and see page 5 paragraphs 61-64. the IP device, element 328 is controlled by the client. Therefore, it is inherent that the IP device receives a TFT information element), wherein setting further comprises setting primary link traffic flow template filter parameters based on the received traffic flow template information element (see figure 3 and see page 5 paragraphs 61-64. the IP device, element 328 is controlled by the client. Therefore, it is inherent that the IP device receives a TFT information element from the client device, which overwrite the previous TFT element).

Regarding claim 3. Donahue discloses a method of controlling packet data traffic where the controlling comprises blocking the incoming packet data from being sent to the wireless device based on a packet data source address being listed as a disallowed source address in the traffic flow template filter parameters (see page 5 paragraphs 61-64. based on the filtering level. Incoming packet will be filtered to block disallowed data from being transmitted to the receiver or client).

Regarding claim 4. Donahue discloses a method of controlling packet data traffic where the controlling comprises blocking the incoming packet data from being sent to the wireless device based on a packet data source address being listed in a range of disallowed data source addresses in the traffic flow template filter parameters (see page 5 paragraphs 59-64. based on filtering level, incoming packet will be filtered to block disallowed data from being transmitted to the receiver or client. The filtering routers are constantly updated to filter data within the range of the disallowed data, depending on the filtering level).

Regarding claim 5. Donahue discloses a method of controlling packet data traffic where the controlling comprises blocking the incoming packet data from being sent to the wireless device based on a packet data source address not being listed as an allowed source address in the traffic flow template filter parameters (see page 5 paragraphs 61-64. data will be blocked based on the filtering level associated with the client. The filtering routers are constantly updated to filter data within the range of the disallowed data, depending on the filtering level).

Regarding claim 6. Donahue discloses a method of controlling packet data traffic where the controlling comprises blocking the incoming packet data from being sent to the wireless device based on a packet data source address not being listed in a range of allowed data source addresses in the traffic flow template filter parameters (see page 5 paragraph 122, the system filters and blocks any data within a disallowed category).

Regarding claim 9. Donahue discloses a method of controlling packet data traffic, which comprises receiving a primary packet data protocol link request message including a traffic flow template information element, an activate packet data protocol context request message identity element (see page 6, paragraph 77. The IP device or the control module is capable of receiving TFT update from the client to update the IP addresses that need to be filtered or blocked), and a requested packet data protocol address element (see page 6, paragraph 77. The IP device or the control module is capable of receiving TFT update from the client to update the IP addresses that need to be filtered or blocked or the associated filtering levels in the IP device), wherein setting further comprises setting primary link traffic flow template filter parameters based on the received traffic flow template information element (see page 6, paragraph 77. the user's update to the IP device to overwrites the previous filtering command. Therefore, the IP device is set based on the last update entered by the user or client).

Regarding claim 10. Donahue discloses a method of controlling packet data traffic where each filter parameter of the primary link traffic flow template filter parameters includes an evaluation precedence identifier (see page 6 paragraph 77. the user indicates which source addresses to be blocked or filtered).

Regarding claim 11. Donahue discloses a method of controlling packet data traffic, which comprises receiving a modify primary packet data protocol link request message, the modify primary packet data protocol link request message including a new traffic flow template element (see page 6 paragraph 77. the user is able to update and change the TFT to include or exclude limitations); and modifying the primary link traffic flow template filter parameters based on the new traffic flow template element (see page 6, paragraph 77. the user's update to the IP device to overwrites the previous filtering command. Therefore, the IP device is set based on the last update entered by the user or client).

Regarding claim 12. Donahue discloses a method in a wireless device of controlling packet data traffic between a wireless network and a wireless device on a primary link. The method comprises sending a primary packet data protocol link request message including a traffic flow template information element (see page 6, paragraph 77. the network user sends a request to update the TFT); and receiving a primary packet data protocol link acknowledgement including an Internet protocol address (inherently, every device get assigned an IP address in order to connect to an IP network. Moreover, when the user updates or configures a gateway or a router, he/she will receive and acknowledgment according to the update requested by the user).

Regarding claim 13. Donahue discloses a method in a wireless device where the primary packet data protocol link request message also includes an activate packet data protocol context request message identity element and a requested packet data protocol address element (see page 6, paragraph 77. The IP device or the control module is capable of receiving TFT update from the client to update the IP addresses that need to be filtered or blocked).

Regarding claim 14. The method disclosed by Donahue further comprises sending a modify primary packet data protocol link request message targeted to a primary packet data protocol link, the modify primary packet data protocol link request message including a new traffic flow template information element (see page 6, paragraph 77. The IP device or the control module is capable of receiving TFT update from the client to update the IP addresses that need to be filtered or blocked).

Regarding claim 15. Donahue a method in a wireless device where the traffic flow template information element includes packet filters for controlling how incoming packet data is sent to the wireless device over the primary link based on comparing incoming packet data against the traffic flow template information element packet filters (see paragraphs 61-64, the user is capable of updating the TFT to suit the his/her network needs. Moreover, the IP device compares IP addresses requested against the TFT to control incoming packets to the wireless device).

Regarding claim 16. Donahue a method in a wireless device where the traffic flow template information element includes packet filters for blocking incoming packet data from being sent to the wireless device over the primary link based on comparing an incoming packet data source address against the traffic flow template information element packet filters (see paragraph 61-64. The IP device (gateway) recognizes the IP address of the wireless device. Thereafter, the IP device decides if the requested content needs to be filtered or blocked by comparing the IP addresses of the requested content and the IP database or the filter level associated with the wireless device).

Regarding claim 17. Donahue a method in a wireless device where the traffic flow template information element includes packet filters for blocking incoming packet data from being sent to the wireless device over the primary link based on comparing an incoming packet data source address against a range of addresses in the traffic flow template information element packet filters (see paragraph 61-64. The IP device (gateway) recognizes the IP address of the wireless device. Thereafter, the IP device decides if the requested content needs to be filtered, blocked or allowed by comparing the IP addresses of the requested content and the IP database or the filter level associated with the wireless device. The filter levels are associated with a range of IP addresses, associated with certain category such as violence or religion, that need to be blocked).

Regarding claim 18. Donahue a method in a wireless device where the traffic flow template information element includes packet filters for allowing incoming packet data to be sent to the wireless device over the primary link based on comparing an incoming packet data source address against the traffic flow template information element packet filters (see paragraph 61-64. The IP device (gateway) recognizes the IP address of the wireless device. Thereafter, the IP device decides if the requested content needs to be filtered, blocked or allowed by comparing the IP addresses of the requested content and the IP database or the filter level associated with the wireless device).

Regarding claim 20. Donahue a method in a wireless device where each filter parameter of the primary link traffic flow template filter parameters include an evaluation precedence identifier (see page 6 paragraph 77. the user indicates which source addresses to be blocked or filtered).

Regarding claim 21. Donahue discloses A network gateway (see figure 2), which comprises a packet data protocol primary link information module (see figure 2, element 204), the packet data protocol primary link information module including traffic flow template information related to controlling which packets of data are sent to a wireless device on a primary link (see figure 3, element 328); and a traffic flow template packet control module coupled to the packet data protocol primary link information module, the traffic flow template packet control module configured to control which packets of data are sent to a wireless device on the primary link based on the traffic flow template information (see page 6, paragraph 77, the user updates the TFT within the IP device to filter or block incoming data).

Regarding claim 22, Donahue discloses A network gateway where the traffic flow template information includes at least one disallowed address for blocking packets of data received from the at least one disallowed address and allowing packets of data from other addresses to be sent to the wireless device (see page 6 paragraph 77, the user updates the list of IP addresses that need to be blocked from reaching the user device. Inherently, other addresses will be sent to the wireless device as long as they are not entered to be filtered).

Regarding claim 23, Donahue discloses A network gateway where the traffic flow template information includes at least one range of addresses for controlling the routing of packets of data received from the at least one range of addresses (see page 6, paragraph 77. the user updates the filtering level that is needed in the IP device. Inherently the level of filtering included a range or a certain category of data that needs to be filtered).

Regarding claim 24. Donahue discloses A network gateway where the traffic flow template information includes at least addresses the at least one address comprising at least one of a universal resource locator address and an Internet protocol address (see figure 3, box 328. the filtering level are associated with content categories. URLs are included in the filter level chosen by the user).

Regarding claim 25. Donahue discloses A network gateway where the traffic flow template packet control module is further configured to receive a primary packet data protocol link request message including a traffic flow template information element and set the traffic flow template information based on the received traffic flow template information element (see page 6, paragraph 77. The IP module is configured to receive updates from the user. The new user update overwrites any previous filter configuration).

Regarding claim 26. Donahue discloses A network gateway where the traffic flow template packet control module is further configured to receive a primary packet data protocol link modify message including a new traffic flow template information element and set the traffic flow template information based on the new traffic flow template information element (see page 6, paragraph 77. The IP module is configured to receive updates from the user. The new user update overwrites any previous filter configuration).

Claim Rejections - 35 USC § 103

6. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

7. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

> invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claim 8 is rejected under 35 U.S.C. 103 (a) as being unpatentable over Donahue in view of Anderson (US 7,171,230).

Donahue discloses a method of controlling packet data traffic where the network gateway comprises a gateway (IP device, figure 2).

Donahue does not specify the gateway used as a gateway GPRS support node. However, Anderson discloses the usage gateway GPRS support node. Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to use the gateway GPRS support node within the network gateway. The motivation for employing the gateway GPRS support node within the filtering system of Donahue being that it will support IP packet transmission to wireless devices such as GSM mobile phones.

10. Claims 7 and 19 are rejected under 35 U.S.C 103 (a) as being unpatentable over Donahue in view of O'Neill (US 2004/0098622).

Regarding claims 7 and 19, Donahue discloses all the limitations of claim 1 and 12.

Donahue does not discloses a method of controlling packet data traffic where the controlling comprises redirecting the incoming packet data from being sent to the wireless device on a primary link based on a packet data source address being listed as a redirection source address in the traffic flow template filter parameters. However, O'Neill discloses a security system where one of the steps of controlling data comprises redirecting the incoming data or packets from being sent to the wireless device. Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to use the packet redirection security step as taught by O'Neill into the packet controlling method of Donahue. The motivation for using the step of redirecting packets as taught by O'Neill into the packet control method of Donahue being that it will redirect packet to another link or network user such as network administrator. For example, the packet redirection can be used to inform or alarm the network administrator that a network user is attempting to access disallowed information within the network.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO_892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mounir Moutaouakil whose telephone number is 571-270-1416. The examiner can normally be reached on Monday-Thursday (4pm-4: 30pm) eastern time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan Kizou can be reached on 571-272-3088. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Mounir Moutaouakil
Art Unit: 2616

HASSAN KIZOU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600